Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

To subscribe to A-ONE, change e-mail addresses, or unsubscribe,
log on to our website at: www.atarinews.org
and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org
and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to
subscribe from.

To download A-ONE, set your browser bookmarks to one of the
following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #0906 02/09/07

~ Net Traffic PCs Hacked ~ People Are Talking! ~ CounterSpy Released!
~ EU Ruling By September ~ Weak Passwords A No-No ~ Dutch Spammer Fined!
~ Teacher Faces Prison! ~ Data Loss Prevention! ~ New Mobile Windows!

~ Firefox Pop-Up Blocker ~ Whistle-Blowers Blown! ~ Super Bowl Virus!

-* MS Internet Security Plan! *-
-* Protecting Yourself Against ID Theft *-
-* Teen Exposure To Internet Porn Is Common! *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"

I have to admit, I'm at a loss for words this week strange as that might seem. Perhaps it's the week-long arctic temperatures freezing my thought processes. I just don't know. So, rather than provide you with the latest chapters in New England weather, or continue my efforts to convince parents to take responsibility for their own kids' actions, I'll take it easy this week by moving immediately forward with this week's issue.

Until next time...

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

[Editor's note: Due to the lack of activity this week, there will be no PAT column this week.]

=~=~=~=

->In This Week's Gaming Section - EA Plans Wii Invasion!
Games Good For Eyes!
Wii Statuettes!
And more!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!

Electronic Arts Plans a Wii Invasion

Video-games publisher Electronic Arts plans to significantly boost its support for Nintendo's Wii game console. In a company earnings report, EA's chief executive, Larry Probst, noted that in the year ahead, the publisher would build on its efforts with the Xbox 360 and the PlayStation 3, but the largest boost would be for the Wii.

EA released only two titles for the Wii console last quarter, with four games released for the PS3 and five for the Xbox 360. Probst noted that about 15 new Wii games were in development.

The game publisher will need to make up some ground over the coming year; EA lost market share during the holiday season, according to analysts.

With the holiday shopping season over, analysts are now watching to see how game developers are honing their title strategies for long-term success. What seems to be occurring is that Microsoft and Nintendo are on one side of the selling battle, while Sony is on the other, noted Forrester Research analyst Paul Jackson.

"Sony is having a hard time," he said. "People who used to bash Microsoft are now going after Sony, and even Microsoft says, 'Don't get a PS3, get an Xbox and a Wii for the same price.'"

Sony appears to have distanced itself somewhat from its gamer audience, Jackson noted, by pricing its console so high. The company had to boost its price tag above competitors because it chose to include more expensive components.

Jackson pointed out that some gamers would rather pay less than shell out for the cutting edge.

The game battle had another salvo this week, when Sony's U.S. spokesperson, Dave Karraker, dismissed the Wii as an "impulse buy," according to news reports.

The use of older, more standard components is doing more than keeping Nintendo's costs down, Jackson said. That tactic is also what is driving developers, including EA, to consider doing more game development for Nintendo, because creating games for less powerful hardware takes less money.

"In the past, Nintendo has typically had the best games coming from in-house, rather than third party developers," he said. "It makes sense, because if you publish your own games, it's more profitable than just getting a licensing fee."

But Nintendo has begun to realize that there are only so many games that can be developed within the company in any given year, Jackson noted. For its part, EA has started to see that the Wii might be the dominant console in the space within the next few years and is eager to cater to a large gamer base.

"Nintendo has done very well in the past two months; they've sold an awful lot of hardware," said Jackson. "They'll build on that, and it's one of

the reasons that EA is looking at them more seriously than in the past."

Study Says Video Games Are Good For Eyes

Video game addicts, rejoice: U.S. researchers have found that playing is actually good for your eyes, and despite all those dire warnings from your parents, it won’t make you blind.

A study by the University of Rochester showed that people who played action video games for a few hours a day over the course of a month improved their vision by about 20 percent.

"Action video game play changes the way our brains process visual information," Daphne Bavelier, professor of brain and cognitive sciences, said in the study published on the university’s Web site, www.rochester.edu, on Tuesday.

"These games push the human visual system to the limits and the brain adapts to it. That learning carries over into other activities and possibly everyday life."

Bavelier and a graduate student tested college students who had played very few, if any, video games in the last year.

Test subjects were given an eye test similar to the one used at regular eye clinics and then divided into two groups - one played shoot-em-up action games for an hour a day while the control group played a less visually complex game. Their vision was tested after the study, with those who played the action game scoring better in the eye test.

The researchers said their findings could help patients with several types of visual defects.

U.S. Artist To Honor Wii Heroes With Statuettes

In the old days, heroes were commemorated with stone statues in public squares.

In today’s video game obsessed society, players can get a Mii.

U.S. artist Paul Thiel is crafting figurines that are replicas of the virtual characters users of Nintendo’s popular console Wii play games with.

Players can customize these characters, called Miis, or they can use caricatures already loaded onto the console. Thiel is now giving Wii fanatics a chance to own them too, according to his friend and agent Allison Q. McCarthy (www.allisonqmccarthy.com).

Thiel created his first Mii sculpture as a Christmas present for McCarthy, who could not stop playing with her Wii, or boasting about her gaming achievements.

"I love to play Wii sports, so naturally it made perfect gift," McCarthy

told Reuters in an email.

The six-inch-tall figurines are made from a type of clay. They are then baked, sanded and hand painted.

"The hair is the toughest bit because it takes the most time to get right," McCarthy added.

Thiel’s Mii has been featured in several gaming and gadget Web sites and magazines. He plans to auction off about five orders for figurines over the Internet from Feb 1.

Atari’s ’Bullet Witch’ Goes Gold

Atari, Inc., one of the world’s most recognized brands and a third-party video game publisher, today announced that development is complete on the neo-apocalyptic action adventure game Bullet Witch. Published in partnership with Japanese publisher AQ Interactive Inc., Bullet Witch is on schedule to ship to stores in North America on February 27th for the Xbox 360 video game and entertainment system from Microsoft and will be available for a suggested retail price of $49.99.

Developed by Japan-based Cavia, Bullet Witch is set on a bleak planet earth in the year 2013 with human kind on the brink of extinction and hideous demons creating a tidal wave of destruction and havoc. All hope of mankind’s survival rests with Alicia, a beautiful witch blessed with magical skills and a swift trigger finger. Players take control of Alicia in her heroic quest to prevent the decimation of mankind through her fearsome weaponry and spectacular powers with which she can manipulate natural phenomena in her environment.

"Bullet Witch flaunts exactly what next-generation gaming is all about with more destructible environments and stunning visual effects, coupled with a captivating storyline," said Jeremiah Cohn, Product Manager, Atari, Inc. "Cavia has made a slew of enhancements in both the European and US versions to deliver an extremely exciting game."

Bullet Witch includes numerous features inspired by American horror and Japanese fantasy monsters. Combining shooting and magic, Bullet Witch will take advantage of Xbox 360’s advanced physics engine by showcasing massive environmental damage, explosions and destruction.

Cavia has balanced and fine tuned gameplay features and made enhancements including improved camera rotation during battle, increased shotgun power, increased Will Power, enemies made more sensitive to attacks, improved enemy AI, and more.

"It’s been a great pleasure for us working on this project with Atari, and we’re very excited about the release of Bullet Witch in North America and Europe," said Naohiko Hoshino, Executive Vice President of AQ Interactive Inc. "How well the critically acclaimed Japanese title will be accepted in the leading countries of Third Person Shooting games is going to be a litmus test, and we consider it a challenge as well. We’ve been working on our upcoming titles high-quality games to the global market in the future."

"Bullet Witch shows a unique world-view with the combination of reality and fantasy through its guns and magical powers," said Tohru Takahashi,

Producer, Cavia Inc. "Also, by using the physics engine, we were able to have glitzy effects in the game as well. We hope players will enjoy Alicia's magical power to blow up cars and enemies and experience all the elements that are impossible in the real world, and we hope the overseas game fans are looking forward to this unique title."

Following launch, players will be able to download additional Bullet Witch content via Xbox Live Marketplace, comprising five packs delivered every two weeks, each containing a new costume for Alicia and revised levels to play through, further adding to the gameplay experience.

For more information on Atari's entire product line-up please visit http://www.atari.com.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

EU Microsoft Judge: Ruling By September

The judge due to rule on Microsoft Corp.'s appeal against the European Commission's antitrust order said Monday he hoped to publish his decision before he leaves office in September.

Bo Vesterdorf, the president of the Court of First Instance, refused to give a precise deadline for his ruling.

"Obviously we would do our very best to get the case out as soon as at all possible," he told reporters at an Informa legal conference in Brussels. "It's a very big case."

Microsoft is challenging the European Union's 2004 antitrust order, which found the software maker broke competition law and fined it a record 497 million euros ($613 million).

To remedy market harms, the EU ordered the company to offer a version of its Windows computer operating system without Microsoft's media player software.

The EU also ordered Microsoft to share communications code and information with rivals to help them develop server software that worked smoothly with the ubiquitous Windows platform.

In July, EU regulators fined Microsoft another 280.5 million euros ($357 million) for failing to supply the "complete and accurate" interoperability required.

Both Microsoft and the Commission can appeal the ruling to one more authority, the European Court of Justice, which is the EU's highest court.

McAfee Dives into Data Loss Prevention

McAfee announced its initial foray into the emerging data loss prevention software market here at the RSA Conference Feb. 5, launching a set of tools to manage the flow of sensitive information across corporate networks and endpoint devices.

Built through a combination of internal development and Santa Clara, Calif.-based McAfee's October 2006 acquisition of Onigma, the package promises the ability for organizations to oversee and control data distribution via a wide range of desktop applications and storage technologies, including e-mail and instant messaging systems, removable USB devices, CD-ROMs, and even printed documents.

The security software maker is pitching DLP (data loss prevention) as a critical piece of its overall corporate risk management strategy, which advocates the use of integrated portfolios of technologies over individual point products and stand-alone applications. McAfee is also hungry to benefit from the rapidly expanding market for DLP tools, growth of which is being driven by an avalanche of high-profile data exposure incidents reported by companies such as retailer TJX Companies.

An occasional well-publicized data breach at a large chain is a terrible thing for that company and its customers, but it just might be a good thing for the industry.

Piloted through a beta project conducted with a small group of companies during the fourth quarter of 2006, McAfee DLP Host combines back-end management server software with a software agent resident on endpoint devices. The combination allows customers to prevent inappropriate data handling both internally and at the network's edge, company officials claim.

The dual-pronged approach is one of the primary differentiators being touted by McAfee's product marketers, who contend that systems that rely too heavily on endpoint management capabilities fail to prevent misuse of information by privileged insiders.

The initial focus of many DLP applications was to protect data from being stolen by employees or network intruders, but software makers competing in the space have begun adopting messages more similar to those pitched by providers of so-called ECM (enterprise content management) tools, but from a dedicated IT security perspective.

While the DLP segment, made up of a handful of smaller developers only several years ago, is quickly becoming crowded with products and vendors, few technologies available today offer a system through which organizations can categorize information on a finite level and create policies for broad sets of data handling permissions, said Vimal Solanki, senior director of product marketing at McAfee.

The more sophisticated approach will allow McAfee to sell the package as both a balm to data security issues and as a compliance automation system to help customers address the growing range of information-protection regulations being passed by government regulators, he said.

"A solution for data loss prevention needs to be where the data resides,

both on the servers and endpoints; we're adopting a philosophy of delivering a solution that sits next to the data wherever it resides and believe it will be well-received by customers," said Solanki. "The technology needs to address the problem effectively whether the worker is in the office, at home or at Starbucks. Ensuring against the loss of data is just another example of how we'll continue to look for opportunities to help companies manage risk."

As part of its DLP rollout, McAfee is releasing a research report created through a survey of more than 300 users at roughly 100 companies about their employers' data handling policies. While 84 percent of the individuals responding to the study said their companies have official guidelines in place to prevent against the exposure of sensitive data, many incidents that violate those policies still occur on a daily basis, according to the research.

For instance, 21 percent of respondents said they have mistakenly left confidential information sitting on a shared printer, 25 percent admitted failure to shred sensitive documents before throwing them away, and 40 percent indicated they take as many as 10 controlled files out of work using printers, USB devices or CD-ROMs.

The innocent nature of those examples points to the need for DLP beyond keeping hackers from stealing data for the purpose of committing crimes such as identity fraud or corporate espionage, McAfee officials said.

"There's a big consideration from the malicious aspects, but data loss prevention is also a huge day-to-day issue, and organizations who don't feel their data is at risk because they've locked down the network from intrusions should worry about accidental loss," Solanki said. "It's not always about a smart hacker. I think everyone has had the experience of sending a message to someone accidentally because their e-mail system filled-in the wrong address; that's the type of situation that can be every bit as dangerous as a data theft, only it happens even more frequently."

Long-Awaited CounterSpy 2.0 Released

At the RSA security conference today Sunbelt Software announced the long-awaited release of CounterSpy 2.0, the consumer-side antispyware utility. CounterSpy incorporates a new technology that Sunbelt calls VIPRE (Virus Intrusion Protection Remediation Engine), as well as boot-time scanning, active protection at the kernel level, and reduced usage of system memory. Version 2.0 is compatible with 32-bit editions Windows Vista.

According to Sunbelt, VIPRE "incorporates both traditional antivirus and cutting-edge antimalware techniques" making it more effective against "today's increasingly complex and blended threats." Rootkits and other deeply entrenched malware are hard to remove because they subvert the operating system itself. Sunbelt's FirstScan technology scans for and removes this type of threat at boot time, before the compromised operating system has even loaded. And the product's Active Protection real-time antispyware operates inside the kernel to block malicious software the moment it tries to launch; it also tracks suspicious program behaviors. Sunbelt is not yet offering support for 64-bit Windows Vista, possibly because 64-bit Vista's PatchGuard makes this type of kernel-level

protection difficult. When 64-bit support becomes available, Counterspy subscribers will receive it as a free upgrade.

The new CounterSpy is smaller and more agile. Specifically, it uses less system memory and creates less of a load on the CPU. Spyware definition updates now just include incremental changes rather than a full download of all definitions, so they download much faster. And at $19.95 the product costs less than Spy Sweeper, Spyware Doctor, and most other competing products. Look for a full report when we've had time to test and evaluate the product.

Microsoft Outlines Internet Security Plan

At the industry's largest information-security conference on Tuesday, Microsoft outlined its Internet-security plans, which include a collaborative effort to strengthen online authentication with the OpenID Framework.

During their keynote address at the RSA Conference, Microsoft Chairman Bill Gates and Chief Research Strategy Officer Craig Mundie discussed how the industry can advance efforts to let people access, share, and use corporate and personal information without fear that it will be compromised.

"Security is the fundamental challenge that will determine whether we can successfully create a new generation of connected experiences that enable people to have anywhere access to communications, content and information," Gates said during the keynote.

The answer for the industry, Gates said, lies in its ability to design systems and processes that give people and organizations a high degree of confidence that the technology they use will protect their identity, their privacy, and their information.

Microsoft stepped up to the plate with a series of announcements it hopes will instill that confidence. These announcements include the Identity Lifecycle Manager 2007, a beta of Microsoft Forefront Server Security Management Console, and support for Extended Validation SSL certificates in Internet Explorer 7.

The software giant also is entering into new collaborations with industry partners.

"To create the level of seamless, pervasive connectivity that will make secure anywhere access a reality, continued collaboration and cooperation across this industry is essential," Mundie said. "If we can work together to enhance trust, it will open the door to a transformation in the way people share experiences, explore ideas, and create opportunities."

According to Gates, advancing trust and enabling anywhere-access requires the industry to focus on three key technological areas: networks, protection, and identity.

Microsoft wants to see networks and the Internet appear and work as if the boundaries between them are seamless, so access for users is easier and faster.

The company also stressed the need for comprehensive security products that integrate seamlessly with each other and are easy to use and manage.

And on the identity front, Microsoft recommended a metasystem based on standard protocols to reduce the complexity of managing identities across networks and the Web.

Microsoft said it is continuing to work with the industry on the WS-* Web standard and with the Interop Vendor Alliance, a global, cross-industry group of software and hardware vendors, to identify opportunities for enhancing interoperability with Microsoft systems.

Microsoft is also collaborating with the OpenID 2.0 specification for use with Windows CardSpace, its application that lets users provide their digital identities in a familiar way. The goal is to offer better protection against phishing attacks without adding complexity to the identity management experience.

"This is good news for end-users," said Charles King, an analyst at Pund-IT. "The Internet is too varied and wonderful to depend on a single vendor for its standards."

Hackers Attack Key Net Traffic Computers

Hackers briefly overwhelmed at least three of the 13 computers that help manage global computer traffic Tuesday in one of the most significant attacks against the Internet since 2002.

Experts said the unusually powerful attacks lasted as long as 12 hours but passed largely unnoticed by most computer users, a testament to the resiliency of the Internet. Behind the scenes, computer scientists worldwide raced to cope with enormous volumes of data that threatened to saturate some of the Internet’s most vital pipelines.

The motive for the attacks was unclear, said Duane Wessels, a researcher at the Cooperative Association for Internet Data Analysis at the San Diego Supercomputing Center. "Maybe to show off or just be disruptive; it doesn’t seem to be extortion or anything like that," Wessels said.

Other experts said the hackers appeared to disguise their origin, but vast amounts of rogue data in the attacks were traced to South Korea.

The attacks appeared to target UltraDNS, the company that operates servers managing traffic for Web sites ending in "org" and some other suffixes, experts said. Officials with NeuStar Inc., which owns UltraDNS, confirmed only that it had observed an unusual increase in traffic.

Among the targeted "root" servers that manage global Internet traffic were ones operated by the Defense Department and the Internet’s primary oversight body.

"There was what appears to be some form of attack during the night hours here in California and into the morning," said John Crain, chief technical officer for the Internet Corporation for Assigned Names and Numbers. He said the attack was continuing and so was the hunt for its origin.

"I don’t think anybody has the full picture," Crain said. "We’re looking

at the data."

Crain said Tuesday’s attack was less serious than attacks against the same 13 "root" servers in October 2002 because technology innovations in recent years have increasingly distributed their workloads to other computers around the globe.

Protecting Yourself Against Online Identity Theft

Internet identity theft is one of the fastest-growing crimes in the U.S. today. For five straight years, the Federal Trade Commission (FTC) ranked it as one of the most-reported types of fraud. Despite the increasing awareness of identity theft among consumers and financial institutions, the identity-theft racket shows no signs of slowing. Reported losses from identity theft, currently responsible for over 40 percent of all fraud complaints, approached nearly $300 million last year.

"True identity theft is a problem that goes far beyond simple credit-card fraud, against which consumers are fully protected, thanks to zero-liability laws and other regulations," says Dave Collett, a spokesperson for MasterCard. "ID theft is when a person’s entire identity is taken over. For that to happen, a fraudster would need far more information than just what is found on a credit or debit card."

All too often, consumers provide that needed information unknowingly through careless Web surfing and by using computers whose security is breached by virus and spyware infections.

One of the leading causes of identity theft online is consumers falling prey to phishing attacks, a form of identity theft that employs a criminal strategy that security professionals call social engineering. Essentially, the process works by tricking e-mail recipients into going to phony Web sites to divulge personal data, like bank-account numbers or credit-card information. Identity thieves also use technical subterfuge through spyware and Trojans to capture user names and passwords so they can gain access to consumers’ financial details.

While many consumers have placed a great deal of faith in their antivirus or antispam software, industry experts say that security applications, for the most part, are not bulletproof as a method for fighting identity thieves. Rather, the software serves mainly to eliminate most major phishing and Trojan threats and works best only in combination with user awareness of increasingly sophisticated social-engineering tactics.

It might seem obvious, but you must be doubly cautious about opening e-mail attachments, which serve as one of the most common vehicles for Trojan horse programs, the worst kind of malware. Just because you recognize the e-mail sender as a family member, friend, or business associate does not make the attachments safe to open. The e-mail might have been sent from a friend’s computer that had been infected with a Trojan-bearing worm.

Network worms, which are arguably the most dangerous of all virus types, jump from one machine to another, spreading around the Internet and leaving infected computers in their wakes. Some network worms do not require any kind of user intervention to spread. They secretly scour the Internet for connected computers that do not have current security

updates or firewalls installed.

Other worms have become so sophisticated that they use multiple strategies to spread themselves. In addition to spreading automatically to computers with outdated security software, these worms can commandeer your e-mail address book and send e-mail messages, laden with Trojans, to your friends and business associates. This means that e-mail recipients have no way of knowing, with perfect certainty, that they are receiving a legitimate message from you or from the worm hiding on your machine.

So, unless you are expecting an e-mail attachment, never assume it is safe to open. Although it might seem tedious, it is important to make sure the attachment is legitimate by checking with the sender before opening it. Once you receive an attachment that looks suspicious, all that is required is a quick reply e-mail asking whether the sender intended for you to receive the file.

Even if your friend intended that you receive the attachment, you are not out of danger just yet. Your friend might have unwittingly forwarded you an infected file, so it is then up to your antivirus or security software to determine whether that attachment is safe to open.

Attached files often contain documents or graphics that can have damaging hidden code in them. Simply clicking on the graphic or a link in the attachment can activate the malicious code, unleashing keylogging programs or other malware designed to steal your identity.

On the surface, many of these messages might seem innocuous. They might contain the latest Internet joke or even a call to help victims of a recent natural disaster. Besides being poor computing etiquette to click the forward button and share these messages with friends and family, doing so can be very dangerous because of the likelihood that they contain malicious links or code.

"It is extremely easy for someone to forge an e-mail message," says Chris Hofmann, director of engineering for the Mozilla Foundation, the organization that makes the Firefox Web browser. "If a message requests that you send your password or other private information, or asks that you run or install an attached file, then it is very likely that the message is not legitimate. When in doubt, just mark the message as junk and delete it."

Beyond exercising a great deal of caution with attachments, it is especially important to use software that not only offers antivirus protection, but also can protect you against spyware and spam. Identity theft comes in many guises. The more types of threats a computer program can detect and deflect, the better.

At the very least, you should use a product that provides advanced e-mail protection and can scan attachments for dangerous content in both incoming and outgoing messages.

Many traditional antivirus vendors now offer integrated-security products that not only give you the ability to set up a firewall easily, but also offer several options for locking down your computer against spam, viruses, and spyware. Rather than require that you purchase and maintain separate software products for each type of protection you need, these integrated software packages combine several kinds of protection in one suite, providing overall security for your computer at a lower cost per module.

McAfee, for example, offers one of the most popular security packages for guarding against virus, spam, and worm attacks. "We've taken a close look at today's threats and found that consumers are facing blended threats more than just one type of malware," says Gus Maldonado, product manager for McAfee. In addition to offering firewall and antivirus protection, McAfee's Internet Security Suite offers protection against phishing.

For a phishing scam to work, you must click the link in a forged e-mail-which might look like it's from your bank or other financial institution-and then enter your user information on the Web page that your browser opens. By adding antiphishing capabilities to your e-mail through McAfee's Internet Security Suite, or any other popular integrated-security package that can protect against phishing, your e-mail program can screen the e-mail source code to help you determine whether the content is legitimate.

McAfee's suite also adds an antiphishing plug-in to your browser so that even if you do click on the link in your e-mail, believing it to be legitimate, you will get another warning when you access the fake Web page. Many integrated-security packages also can alert you if your browser is being secretly redirected to a known or suspected phishing Web site or when secret executables, such as malicious ActiveX controls (which are Internet Explorer plug-ins that add all kinds of functionality), attempt to transfer your personal information to another computer on the Internet.

One of the most common methods that antispyware and antivirus software uses to identify malicious code and remove it is by comparing what it finds on your hard drive - or what comes in via e-mail - to an exhaustive database of malicious threats. Users who keep clicking the delay button instead of following through with their software's regular suggestions to update their local signature list can put themselves at risk.

While some of the most advanced security software uses "heuristics" - a method that relies on looking at the actual behavior of malicious code to determine whether it might be attempting to create a viral infection-the mainstay of any antivirus application is its database of signature files. An out-of-date database can weaken your security software's protective barrier and make it much easier for thieves to steal your identity. So it is imperative that your security software always use the most recent signature files available from your security vendor.

Of course, your software might want to update itself right when you're in the middle of doing something on your PC that requires most of your processor's power. And you might be tempted to click the delay button. But when the software prompts you to update, resist the urge to postpone it. The more current your software is, the less likely it will be that you have to cancel your credit cards as a result of identity theft.

It also is important to learn about the settings for your security software's update features. Some programs will let you choose a time interval for regular updates. Other programs provide an option to do it automatically. In most mainstream security software, these settings are relatively easy to find.

In much the same way that the software gives you the ability to schedule software updates, most popular security packages give you the ability to schedule complete system scans for intruders. While these scans often slow the responsiveness of other programs that you might be running at the time, you should avoid the temptation to cancel a scan just because it is inconvenient. Also, it is very important to scan your computer regularly.

Having the ability to detect and remove harmful viruses and spyware that can steal your identity is worthless if your software does not run frequently enough to keep you protected.

As a routine safe-computing practice that can help avoid many kinds of identity-stealing scams, you should always enter a Web site's URL in a new browser window. For example, if an e-mail claiming to be from your bank asks you to log in to verify your password or account information, resist the temptation to click on the link in the e-mail itself, regardless of how authentic the message might appear.

Do not be fooled by these common tricks. One of the most effective methods that phishers use is to send an e-mail that looks exactly like the one you would get from your bank, service provider, or just about any kind of company that has your sensitive financial information. While these pieces of e-mail might look legitimate, they secretly hide fake URLs and potentially malicious script in the HTML source code.

Here is one example of the kind of messages designed to steal your account information: "This e-mail is a reminder that your eBay account information is suspended. To avoid any interruption to your service, including the ability to log on to your eBay account, please update your credit or debit card information by clicking here and submitting our form." While the text might sound completely authentic and the e-mail might look perfectly legitimate, replete with eBay graphics, resist the temptation to follow the instructions.

In many cases, the actual link in the HTML code will be different from the URL displayed in the e-mail. In other words, even if the piece of e-mail looks legitimate and a link in it claims to take you to a familiar and legitimate URL, the underlying source might send you to an impostor Web page that looks exactly like eBay but is designed to steal your personal information or bank account number. However, if you copy and paste the included link into a new browser window - or if you simply type the URL in that window yourself - you can avoid this kind of trickery altogether.

Over recent years, Microsoft's Internet Explorer 6 was targeted and hit by numerous attacks, primarily because it has been the most widely used Web browser. When it comes down to it, it's a numbers game for hackers. They know that some 90 percent of Internet users rely on Internet Explorer to surf the Web. So they tailor their malicious scripts, ActiveX controls, and all sorts of other malware specifically to weaknesses in the current version of Internet Explorer.

Fortunately, Internet Explorer 7 (IE7) is now available with a much improved security arsenal to help protect against online scams. The IE7 Web browser has built-in antiphishing features designed to alert you when you've hit a fraudulent site. When you surf the Web with the IE7 browser, antiphishing is turned on by default. Each Web site you visit is checked against a database maintained by Microsoft, and known frauds are blocked.

There are also several alternative browsers that can take you out of the targeted majority. And there are several add-on security tools that can make life with Internet Explorer much more secure.

The Firefox 2.0 browser, for example, has two antiphishing options. The sites you visit can be checked against a local database on your computer or against a live database maintained by Google. Earthlink's ScamBlocker can also compare the URLs you are browsing against a known list of fraudulent Web sites and Web sites that are known to install malicious

code on visitors' computers. These programs either block your connection to the Web site altogether or issue a warning before loading the page.

Some e-mail clients provide similar antiphishing features. For example, the Mozilla Foundation's Thunderbird e-mail client detects links in e-mail that use Internet Protocol addresses instead of domain names and other common techniques for diverting users to an attacker's Web site. When Thunderbird detects this content in messages, it displays a status bar at the top of the message to indicate the message might be an e-mail scam.

While Internet Explorer and alternative browsers have battened down the security hatches quite a bit, all-in-one security software may still be your best bet for fighting identity theft on the technology front. But installing an integrated-security package does not mean that you do not need to exercise caution against online scams.

Beyond security software and good common sense when it comes to transacting business online, it is important to watch your credit information. Truly nasty identity theft not only hits you in the pocketbook, but also can affect your credit. In fact, watching your credit is a great way to ensure that you haven't been a victim of identity theft. You can obtain free credit reports from the major credit-reporting services, like Experian or Equifax. For a relatively small price, however, a credit-monitoring service can notify you immediately about any suspicious transactions that would affect your credit information.

For example, Equifax, one of the three leading credit bureaus, offers a service called Credit Watch that can alert you about any credit file changes at all three major credit-reporting companies. Other credit-monitoring services include Identity Guard, which provides three-bureau monitoring and is offered directly through some online-banking outlets. Another is TrueCredit, which provides reports on credit scores from the three major credit bureaus and offers other credit-monitoring services.

You also should check with your existing credit-card companies to make sure you are not charged for fraudulent activity resulting from identity theft. If the banks backing the credit cards do not provide this service, consider closing those accounts and opening new ones with banks that provide better protection. In the process, another step is to activate credit-card insurance through the account sponsors or purchase credit-card insurance from a credit-monitoring service.

Being well armed with information about computer security is just as necessary as having up-to-date software. Find out all you can to minimize your chances of becoming an identity-theft victim. Educating yourself about these threats is easier than you might think. Most banks and financial institutions now provide their subscribers with information about privacy and identity-theft issues.

Be sure you familiarize yourself with your bank's procedures for protecting yourself against identity theft. For instance, PayPal will never send an e-mail addressed to "Dear PayPal User." Instead, PayPal always uses your first and last names, two pieces of information that identity thieves will not necessarily know until you tell them.

Also, an easy way to spot a fraudulent e-mail message is to move the mouse pointer over the link in a suspected phishing e-mail. In most cases, you will see the details of the actual URL that the link goes to. Usually,

phishing e-mail contains lengthy Web addresses that are not based on your bank’s domain name. However, it’s also important to be on the lookout for some very sophisticated phishing scams that use advanced scripting to mess with your e-mail client’s ability to determine the real link.

You can learn more about protecting yourself from phishing attacks and other online identity scams by visiting sites specifically devoted to these issues, such as www.antiphishing.org and www.consumer.gov/idtheft.

Ultimately, while technology can help protect you, the fight against identity theft must be fought with common sense, informed caution, and a solid understanding of what you are up against.

Pop-up Blocker Problem Found in Firefox

A flaw in the pop-up blocker of the open-source browser Firefox could allow an attacker to access local files, according to security analysts.

The flaw, however, does not affect Firefox 2.0, the latest version of the browser, but version 1.5.0.9, according to Beyond Security, which credited the find to Michal Zalewski.

The attack could occur if a user manually allows a pop-window to appear. The browser normally blocks access to local files, but when a pop-up is manually allowed, "normal URL permission checks are bypassed," Beyond Security said.

To make the hack work, however, a malicious file containing the exploit code would have to already be on the system, the advisory said. The file could be planted on the system by enticing a user to click on a link that would download the file.

The malicious file could then enable access to other files, which could be transferred to a remote server. Mozilla Corp., the distributor of Firefox, could not immediately comment on the report.

Weak Passwords Really Do Help Hackers

Left online for 24 days to see how hackers would attack them, four Linux computers with weak passwords were hit by some 270,000 intrusion attempts - about one attempt every 39 seconds, according to a study conducted by a researcher at the University of Maryland.

Among the key findings: Weak passwords really do make hackers’ jobs much easier.

The study also found that improved selection of usernames and associated passwords can make a big difference in whether attackers get into someone’s computer.

The study was led by Michel Cukier, an assistant professor of mechanical engineering and an affiliate of the university’s Clark School Center for Risk and Reliability and Institute for Systems Research. His goal was to look at how hackers behave when they attack computer systems - and what

they do once they gain access.

Using software tools that help hackers guess usernames and passwords, the study logged the most common words hackers tried to use to log into the systems.

Cukier and two graduate students found that most attacks were conducted by hackers using dictionary scripts, which run through lists of common usernames and passwords in attempts to break into a computer.

Some 825 of the attacks were ultimately successful and the hackers were able to log into the systems. The study was conducted between Nov. 14 and Dec. 8 at the school.

Cukier was not surprised by what he found. "Root" was the top guess by dictionary scripts in about 12.34% of the attempts, while "admin" was tried 1.63% of the time. The word "test" was tried as a username 1.12% of the time, while "guest" was tried 0.84% of the time, according to the experiment’s logs.

The dictionary script software tried 43% of the time to use the same username word as a password to try to gain entrance into the affected systems, Cukier said. The reason, he said, is that hackers try for the simplest combinations because they just might work.

Once inside the systems, hackers conducted several typical inquiries, he said, including checking software configurations, changing passwords, checking the hardware and/or software configuration again, downloading a file, installing the downloaded program and then running it.

For IT security workers, the study reinforced the obvious. "Weak passwords are a real issue," Cukier said.

At the University of Maryland, users are told that passwords should include at least eight characters, with at least one uppercase letter and one lowercase. The school also recommends that at least one character be a number or punctuation symbol, Cukier said. All passwords should be changed every 180 days, according to the university’s recommendations.

"That’s really reasonable," Cukier said of the guidelines. "It’s not helpful if the password is so complicated that people don’t remember it and [therefore] write it down on a sticky note next to their computer."

Users can use the title of a favorite book for a password or even the first letters from a memorable sentence, he said. "They’ll be easy for you to remember because you’ll be able to remember the sentence... without having to write it down," Cukier said.

Microsoft Presents New Windows Mobile Version

Microsoft unveiled on Thursday a new version of its Windows operating system for mobile devices, making it look more like Windows Vista and adding features previously only available on personal computers.

Called Windows Mobile 6 and available in the second quarter of 2007, it introduces the ability to view e-mails in their original HTML Internet format with live Web links from advanced mobile phones, generally

referred to as smartphones.

Windows Mobile 6 also includes Windows Live, which allows instant messaging with more than one person at a time and can send a file or image, or record and send voice notes.

Windows Mobile 6 users can also view, navigate and edit documents in the original Word, Outlook, Excel and Powerpoint format, without affecting tables, images or text.

Windows Mobile 6 also has new security features.

Microsoft last week introduced Vista, the new version of its personal computer operating system.

Despite its modest global market share, well behind software from Symbian and Nokia, Microsoft's Windows Mobile was selected by Vodafone in November as one of only three mobile operating software systems it would support in the long run. The other two were Symbian/Nokia Series 60 and Linux.

The software giant has said sales of mobile phones running on Windows Mobile would double this fiscal year to mid-2007 and are set to double again in the year beyond.

Whistle Blown On Wiki Site For Whistle-Blowers

It had to happen. A Web site set up to encourage anonymous leaks of controversial government secrets has been exposed before its launch.

Government insiders around the world will be invited to use the site as cover to leak evidence of corruption and injustice. It is meant to be an adaptation of Wikipedia, the popular online encyclopedia, to encourage whistle-blowers to come forward.

Depending entirely on voluntary contributions for its content, http://www.wikileaks.org will officially go live in a few months: instead of the public submitting entries, it is asking officials to publish state documents.

"What conscience cannot contain, and institutional secrecy unjustly conceals, Wikileaks can broadcast to the world," reads the answer to one of its Frequently Asked Questions.

"Wikileaks will be the outlet for every government official, every bureaucrat, every corporate worker, who becomes privy to embarrassing information which the institution wants to hide but the public needs to know."

However, the first major leak at Wikileaks was a textbook example of the viral, or word-of-mouth, marketing that sets the Web buzzing: the site itself was the target.

Wikileaks had, its developers said, wanted to maintain a low profile in its development stage. For example, the "adviser" who spoke to Reuters on behalf of the site did so on condition of anonymity.

But a blogger, John Young, blew the lid on the project.

Other bloggers and media including Time magazine have since exposed James Chen and Julian Assange, two of the project developers, in a cocktail of information and speculation that highlights the Web's perils for the factfinder.

Some bloggers have speculated the site could be a front for the U.S. Central Intelligence Agency. Others just dismissed it as laughably amateurish.

If they were surprised, the site's developers did not seem concerned by the fact that they had been rumbled.

"This is clearly a project whose time has come because the response has been overwhelming and very positive," said the woman who contacted Reuters by phone, calling herself a member of the Wikileaks' advisory board.

The Web site says it counts Chinese dissidents among its international team of founders, and some of its advisers are Russian and Tibetan refugees.

Despite the initial hitch, its developers say it will be secure and its contributors untraceable, allowing people to publicize wrongdoing without fear of being found out.

"We want to instill bravery in whistle-blowers," the Wikileaks adviser said. It says it has already received 1.2 million separate leaked documents.

If the site launches, it would not be the first time the Internet had been used by officials to draw attention to malfeasance.

Just last month, former Kenyan anti-corruption chief John Githongo posted an audio tape online that he said showed government ministers pressuring him to drop an investigation.

There are also established Web sites, such as John Young's http://cryptome.org and http://www.thesmokinggun.com, that feature potentially controversial documents.

However, Wikileaks says it wants to be a "central clearing house" for such leaks. And, taking to new heights the current Web vogue for crowd-sourcing - encouraging users to contribute - it says it will take a "democratic" approach to verifying the information.

Anyone will be able to comment on the importance - and judge the authenticity - of the whistle-blowers' submissions.

"Instead of a couple of academic specialists, Wikileaks will provide a forum for the entire global community to examine any document," it says.

The hope is that communities of experts will cluster around the site: "If a document is leaked from Somalia, the entire Somali refugee community can analyze it and put it in context."

Analysts say high standards will be needed to ensure documents on the site are not distortions of the truth or out-and-out lies - a prospect raised by the anonymity granted to the sources.

"It's problematic because it's going to be the preferred cloak of a malicious person," said Guy Dehn, director of Public Concern at Work, an

advocacy group for whistle-blowing in Britain.

The "democratic" vetting process may not help.

"Lots of people like a salacious rumor and may not care whether an expert thinks it’s true or not, and it may cause substantial damage in the interim," said John Palfrey, a Harvard University professor specializing in international law.

Even if potential legal problems were addressed, Dehn said encouraging anonymity could have other harmful consequences.

Public debate might shift from the substance of the leak to the identity of the whistle-blower. "Whistle-blowing works when it is done openly," Dehn said. "That’s what helps drive the accountability."

Dutch Man Fined $97,000 For 9B Spam

A spammer whom authorities say e-mailed more than 9 billion unwanted advertisements for products like erection pills faces a hefty fine: If he needs headache medication or debt relief there’s probably an unsolicited ad in his own inbox.

Dutch authorities have levied a $97,000 fine on an unidentified man for sending "unsolicited electronic messages to consumers to promote erection enhancement pills, pornographic web sites, sex products and such," the country’s telecommunications watchdog said Friday in a statement. It was the largest such fine levied by the watchdog, known by its Dutch acronym OPTA.

OPTA said it considered several factors, including the sheer volume of the messages, saying the 9 billion was a "minimum" estimate.

"Another aggravating factor was that this person used hundreds of so-called proxies," OPTA said. That’s a common spamming technique in which computers of unsuspecting users are commandeered, often using viruses or other malicious software, to conceal the messages’ true origins, making them more likely to slip by anti-spam filters.

Authorities say the man earned at least $52,000 from sending the spam in the year before he was caught on Nov. 1, 2005.

The spammer had argued in his defense that he had already stopped sending spam by the time he was caught, "not because he realized that what he was doing was a violation of the law, but because he simply wasn’t earning enough money by sending the messages," OPTA said. The Netherlands outlawed spam in May 2004.

OPTA said Microsoft Corp. had helped in its investigation by gathering evidence.

Super Bowl Virus Spreads

Security experts are finding an increasing number of Web sites hosting

malicious JavaScript code first detected on Super Bowl-related sites last week.

Sites covering topics ranging from health care to government have been hacked to host the JavaScript, SANS Internet Storm Center Director Marcus H. Sachs wrote on the SANS blog, listing some of the hacked sites.

"System administrators might want to check their network flow logs for any traffic to these sites and for any traffic to the five sites that hosted the hostile JavaScript," Sachs wrote.

The attack targets two known vulnerabilities in Microsoft Windows, for which Microsoft introduced patches in April and in January.

Computers with unpatched software are vulnerable to the attack. If one of the hacked sites is visited, the JavaScript code directs the browser to a second Web server, based in China, and tries to install a Trojan Horse downloader and password-stealing program on the victim’s computer.

Initially, the exploit appeared isolated to Web sites related to U.S. football, as hackers tried to capitalize on the surge of traffic to sites concerning the Super Bowl sporting event, which was played on Sunday. The site of the Miami Dolphins team, and another site for its stadium, were hacked, although they were eventually cleaned up.

Security company Websense reported the problem on the stadium site on Friday. Websense recommended users stay away from the affected sites until they had been cleaned up.

Teen Exposure To Online Pornography Common

About four in every 10 U.S. youngsters age 10 to 17 report they’ve seen pornography while on the Internet, two-thirds of them saying it was uninvited, according to a study published on Monday.

Many of the encounters with online pornography, both sought-out and accidental, were related to use of file-sharing programs to download images, the report from the University of New Hampshire in Durham said.

"Although there is evidence that most youth are not particularly upset when they encounter unwanted pornography on the Internet (it) could have a greater impact on some youth than voluntary encounters with pornography," the study said.

"Some youth may be psychologically and developmentally unprepared for unwanted exposure, and online images may be more graphic and extreme than pornography available from other sources," it added.

The report, published in the February issue of Pediatrics, the journal of the American Academy of Pediatrics, was based on a telephone survey made of a representative sample of 1,500 U.S. youngsters from March to June, 2005.

In all 42 percent reported having been exposed to online pornography in the 12 months before they were questioned. Of that group 66 percent said they were not trying to find the material when they encountered it, which happened sometimes because of misspelled Web addresses, pop-up

advertisements or spam e-mails.

The remaining third who said they sought out pornography were more likely to be teen-aged boys who also used file-sharing programs to download images, talked online to strangers about sex, used the Internet at friends' homes, or possibly suffered from depression.

The researchers said sexual curiosity is normal in the teen years "and many might say that visiting X-rated Web sites is developmentally appropriate behavior." But they said some experts are worried that it could undermine social values or attitudes about sexual behavior, lead to promiscuity or compulsive and deviant behavior.

Doctors, teachers, parents and others "should assume that most boys of high school age who use the Internet have some degree of exposure to online pornography as do many girls," the study concluded.

Teacher Faces Prison for Pop-Up Infested PC

Have you ever faced a pop-up that wouldn't go away? You try clicking it closed and another pops up in less than a nanosecond. You reboot the system, annoyed that your anti-spyware program let something slip through.

That's a hassle, sure - but chances are, your experience won't land you in jail.

Julie Amero, a substitute teacher in Norwich, Connecticut, has been convicted of impairing the morals of a child and risking injury to a minor by exposing as many as ten seventh-grade students to porn sites.

It's a short story: On October, 19, 2004, Amero was a substitute teacher for a seventh-grade language class at Kelly Middle School. A few students were crowded around a PC; some were giggling. She investigated and saw the kids looking at a barrage of graphic, hard-core pornographic pop-ups.

The prosecution contended that she had used the computer to visit porn sites. The defense said that wasn't true and argued that the machine was infested with spyware and malware, and that opening the browser caused the computer to go into an endless loop of pop-ups leading to porn sites.

Amero maintains her innocence. She refused offers of a plea bargain and now faces an astounding 40 years in prison (her sentencing is on March 2).

I'll admit all my don't haves right away: I don't have access to court records; I don't have first-hand evidence of what occurred; and I haven't examined the computer's hard drive myself.

What I do have is a working knowledge of spyware and plenty of experience cleaning infected PCs.

I also have a copy of the report written by computer forensic specialist W. Herbert Horner, the expert witness who testified in Amero's defense. You can read it, too; it's on the NetQos site.

Horner made an image of the computer's hard drive. He saw that there was no firewall and that the antivirus program was outdated. He also found 42 active "spyware/adware tracking cookie/programs." Most important, Horner

said that 27 of the spyware apps were accessed before Amero had access to the computer.

To me, the implication is clear that Amero hadn’t used the PC for browse for porn, as the prosecution claimed.

The defense wanted Horner to have Internet access at the trial in order to re-create what happened to Amero in the classroom. The prosecution objected, claiming they hadn’t had ?full disclosure? of Horner’s examination.

In my opinion, had the defense attorney been on his toes, and had the jury seen the demonstration, Amero would have been found innocent.

The question is, Who should be held responsible? After reading articles in the Norwich Bulletin, the area’s local newspaper, and a chat with someone familiar with the case, I’ve come to some conclusions. (And if you’ve ever helped a computer novice deal with a PC loaded with spyware, I think you know who I’m siding with.)

First, it would be a good idea to take a look at newspaper articles covering the trial. Read the January 5, 2007 article, the next on January 7, and the January 11 editorial supporting the conviction.

Now, back to our story. To begin with, the prosecutor pointed his finger at Amero because she didn’t turn off the computer right away.

If I faced the same situation, I’d probably panic, just as Amero did - shield the kids from seeing the monitor and move them away from the computer. Then I’d reach over to an unfamiliar system, fumble around looking for the Off switch, and turn off the monitor, or computer, or both.

I imagine Amero was also flustered because she was told by the class’s regular teacher, quite adamantly, not to turn off the computer. That’s a lame excuse, I agree, because questioning authority is sometimes the right thing to do.

But I’ve learned from my source that Amero is a rank novice. About the most she can do is check e-mail on AOL using her husband’s home computer. That says lots, no?

For instance, when faced with the classroom PC’s pop-ups, her reaction was to click the red "x" in the corner of each box - which, as anyone who’s faced spyware knows, often results in another pop-up.

More important, though, if the school had done its part in protecting its students, it would have up-to-date anti-spyware and antivirus programs installed on every PC.

On January 24 the Norwich Bulletin reported that the school district’s technology administrator, Information Services Director Bob Hartz, said, "from August to October 2004, the district’s filtering system didn’t regularly add newly discovered pornographic sites to its restricted Web sites database." Oddly enough, they upgraded the software just after Amero’s incident.

In my opinion, Amero is the victim here.

The blogsphere has been following the story carefully, though the

mainstream media hasn’t picked it up yet. My guess is when it does, the bits will hit the fan.

Have you ever clicked on a browser message that looks legit and offers to, say, block spam or remove spyware? According to Sunbelt Software’s spyware expert Alex Eckelberry, if you click on an innocent looking dialog, you could inadvertently install malware on your machine and end up with a PC that’s infested with annoying pop-up ads that appear whenever you open your browser. Watch this YouTube video to see exactly how it happens.

To protect yourself from spyware, you need protection and advice - like you can get from PC World’s Spyware & Security Info Center. But you may just want to cut to the chase. In that case, read "Spyware Fighters," "Disarm Net Threats," and "First Look: SiteAdvisor Plus vs. Norton Confidential."

=~=~=~=